NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ARCHITECTING THE SAFETY ASSESSMENT OF LARGE-SCALE SYSTEMS INTEGRATION

by

Tong Choon Yin

December 2009

Thesis Advisor:	Eugene Paulo
Second Reader:	Mark Rhoades

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Architecting the Safety Assessment of Large-scale Systems Integration		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Tong Choon Yin			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

This research identifies the information/data required to perform a safety assessment for large-scale systems integration. From these required safety-related information/data, and the utilization of system engineering processes and practices, a safety assessment architecture is developed. As a result, the risk of known hazards is mitigated to as low as reasonably practical (ALARP) and the system health of these large-scale system integrations is improved throughout the system's life cycle.

The thesis first identifies the current gap in system safety assessment for large-scale system integrations, especially in the area of Commercial of the Shelf (COTS) and Non-Developmental Item (NDI) systems integration. Next, with reference to the DoD system life cycle process, a COTS/NDI system integration life cycle process model is proposed. In addition, in line with the DoD policy to have a joint weapon system safety review board, a system safety functional hierarchy is then created. Using the functional hierarchy created, more detailed sub-functions and measures of effectiveness for system safety assessment are then analyzed.

Finally, a hazard list table is proposed as a tool to be used in relation to the system safety assessment functional hierarchy so as to achieve the objective to identify, mitigate, trace and accept all residual risks associated with the large-scale system integration throughout its life cycle. A case example of the Harpoon Weapon System (HWS) safety assessment on a ship platform is used to further explain the usage and process of generating, maintaining and tracking the hazard list table.

14. SUBJECT TERMS Systems Integration, System Safety, System-of-Systems Safety			**15. NUMBER OF PAGES** 75
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ARCHITECTING THE SAFETY ASSESSMENT OF LARGE-SCALE SYSTEMS INTEGRATION

Tong Choon Yin
Defence Science & Technology Agency
B.S., Nanyang Technological University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEM ENGINEERING AND ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
December 2009

Author: Tong Choon Yin

Approved by: Eugene Paulo
Thesis Advisor

Mark Rhoades
Second Reader

Clifford A. Whitcomb
Chairman, Department of System Engineering

Robert F. Dell, PhD
Chairman, Department of Operations Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research identifies the information/data required to perform a safety assessment for large-scale systems integration. From these required safety-related information/data, and the utilization of system engineering processes and practices, a safety assessment architecture is developed. As a result, the risk of known hazards is mitigated to as low as reasonably practical (ALARP) and the system health of these large-scale system integrations is improved throughout the system's life cycle.

The thesis first identifies the current gap in system safety assessment for large-scale system integrations, especially in the area of Commercial of the Shelf (COTS) and Non-Developmental Item (NDI) systems integration. Next, with reference to the DoD system life cycle process, a COTS/NDI system integration life cycle process model is proposed. In addition, in line with the DoD policy to have a joint weapon system safety review board, a system safety functional hierarchy is then created. Using the functional hierarchy created, more detailed sub-functions and measures of effectiveness for system safety assessment are then analyzed.

Finally, a hazard list table is proposed as a tool to be used in relation to the system safety assessment functional hierarchy so as to achieve the objective to identify, mitigate, trace and accept all residual risks associated with the large-scale system integration throughout its life cycle. A case example of the Harpoon Weapon System (HWS) safety assessment on a ship platform is used to further explain the usage and process of generating, maintaining and tracking the hazard list table.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I would like to thank Professor Eugene Paulo for his mentorship during the course of this research and throughout my graduate studies.

In addition, I would like to express my gratitude to both CDR Doug Burton (Chair, Applied Systems Analysis and SEA Program Officer) and Professor Mark Stevens (SEA Academic Associate) for their guidance and advice provided throughout the System Engineering Analysis curriculum, which made my graduate studies at the Naval Postgraduate School a memorable and exciting experience.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Ideally, end users would be involved in all phases (from development to operation) of their systems such that a thorough safety assessment can be performed and associated hazard risks tracked through the systems' life cycle. However, a majority of countries rely on the defense market (Foreign Military Sales [FMS] or commercial off-the-shelf [COTS]) to acquire proven systems and then perform certain levels of adaptation in order to integrate these COTS systems with their combat platforms.

As a result, the safety assessment for such COTS or Non Developmental Items (NDI) systems installation onboard various types of combat platforms is usually performed without consideration of overall integration of the system with the major combat platform. As the complexity of system integrations increases, there is an increasing need for system architecture to be developed in order to consolidate the various standalone safety assessments and then identify the overall hazard risks associated with their corresponding mitigation factors for such large-scale systems integration. The development of safety systems architecture is the focus of this thesis.

Using a case example of the Harpoon Weapon System integration on a foreign armed forces' combat platform, the following gaps were identified when conducting safety assessment for large-scale system integrations:

a. Most end users (i.e., foreign armed forces) could only obtain safety assessments for a standalone weapon system and are not able to address the overall assessment of an integrated system to achieve their needed capability.

b. As the complexity of system integrations increased, changes or upgrades being done in one system will affect the overall system safety and there will be a need to review the entire system safety assessment. There is currently no identified process that could allow tracking and monitoring of all changes in large-scale system integrations.

c. The rapid and more organized threat emergence in recent years has led to the constant review of each nation's concept of operations (CONOPS), directly affecting how systems are to be operated, which leads to the changes in the probability of hazard occurrence and their associated consequences.

While the main benefit of COTS acquisition is savings on research and development costs and risk reduction associated with new development, it poses other challenges and pitfalls. These include limited changes to the basic design and changes not controlled by the end user. COTS further limits the end user in obtaining information about the developmental phases and hence may not allow full awareness of the problems identified and methodology to resolve them.

The system life cycle process model for a large-scale systems integration is seen in Figure 1. Most foreign armed forces obtained their systems in milestone B; this essentially means that about one-third of the system safety information resided in the OEM or that most of the time this information is non-releasable due to classification restriction (i.e., security and economics aspects). In summary, the system safety assessment of large-scale systems integration can be broken into the following areas of focus during its life cycle:

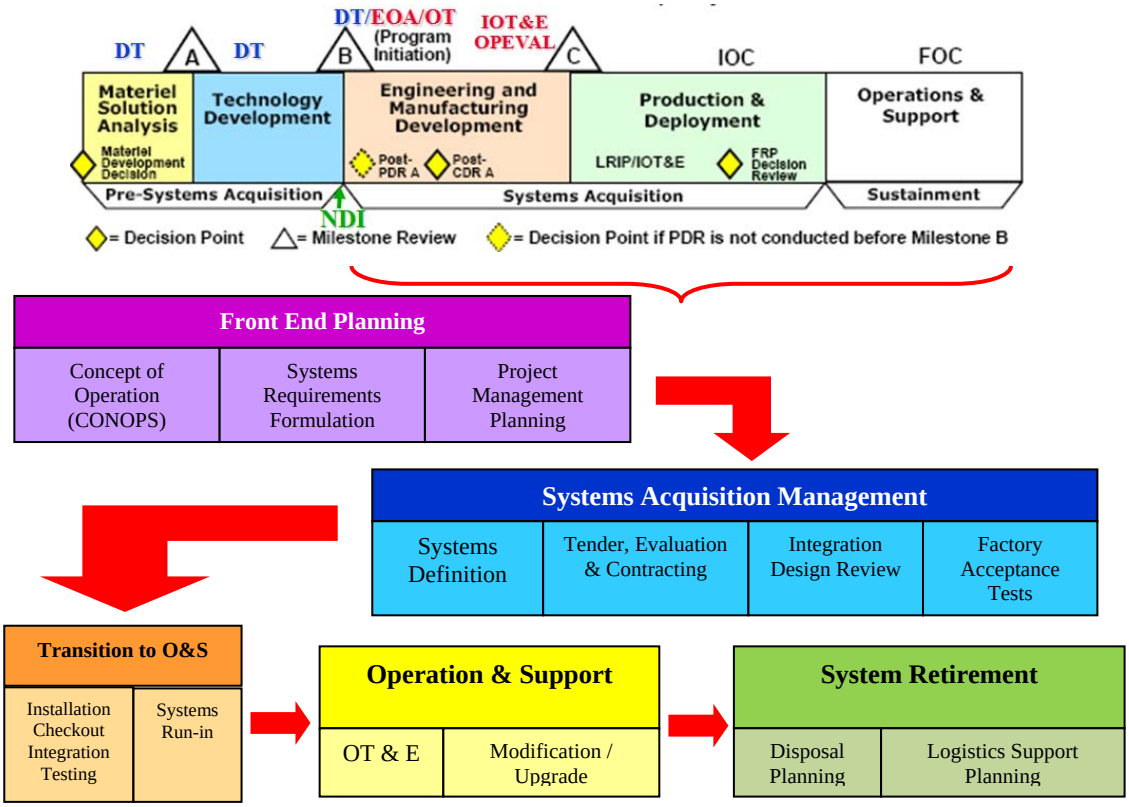


Figure 1. System Life Cycle Process Model for NDI/COTS (After: [21])

- **Safety to Interfacing Platform** – This should cover system safety in relation to the interfacing platform on which all the systems are to be operated.
- **Safety to Personnel** – This concentrates on the day-to-day handling and operation of the systems by trained operators.
- **Safety Template Optimization** – When there are two or more integrated weapon systems, there is high possibility of overlapping weapon damage areas or violation of weapon safety templates of boundaries. In general, the safety template for each weapon or missile is generated based on its associated guidance error, other environmental and weapon system consideration and certain assumptions on the area of operations for the country of origin.

In order to formulate an integrated system safety assessment, it is important to first describe the essential functions that are required to fulfill this object. Figure 2 depicts the proposed four main functions critical to a large-scale systems safety assessment. Finally, a case example of the Harpoon Weapon System (HWS) safety assessment on a ship platform is used to further explained the usage and process of generating, maintaining and tracking the hazard list table.

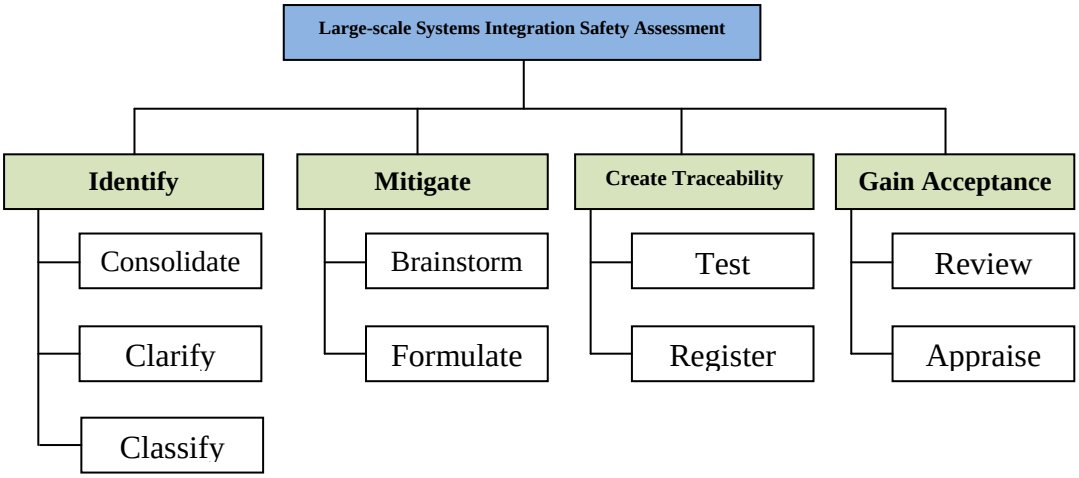


Figure 2. System Safety Assessment Functional Hierarchy

a. **Identify** – This represents the ability to consolidate, clarify and classify all risks and hazards within the large-scale systems, where much of the data collection and consolidation of different system safety reports from the various sub-systems within the large-scale systems architecture is conducted. Next, clarification of each sub-system's OEM on their safety

report and basis of their safety hazards should be conducted so that the team will be able to understand the assumptions taken in deriving the residual risks.

b. **Mitigate** – This seeks to brainstorm and formulate all possible mitigation factors in order to reduce these hazards to "as low as practically reasonable." This is a highly iterative process and involves various SMEs and the tight coordination of the Integrated Program Management Team (IPMT).

c. **Create Traceability** – From the test cases formulated in the Mitigate function, a database or table of identified risks, described as a Hazard Listing, and its associated mitigation measures should then be created, maintained and tracked conscientiously throughout this whole process. Information in this database should include details such as description of risk, source of risk, affected interfacing systems, initial risk level, consequences, mitigation measures and mitigated/residual risk level.

d. **Gain Acceptance** – This involves reviewing the residual/mitigated risk and appraising all stakeholders on the acceptance of all safety hazards associated with the large-scale systems integration. In addition to the Hazard Listing, a risk assessment matrix should also be developed to better represent the associated residual risks in relation to the probability of occurrence, which is dependent on the concept of operations.

In summarizing the findings gathered in this research, the following guideline and/or checklist attempts to provide a quick overview and template necessary in order to kick-start the system safety assessment:

a. **Determining the Lead System Safety Assessment (aka System Integrator)** - In order to fulfill the need for a joint weapon safety oversight, it is important first to identify which sub-system within the large-scale systems will be the lead system. Generally, in most cases the logical candidate for the lead system is the weapon system, if it is the only weapon system within the large-scale systems integration, due to its greater risk exposures with higher hazard consequences.

b. **Review of Safety Assessment Matrices** - Due to the complexity of the large-scale systems integration of COTS/NDI, there could be a possibility that the Probability of Occurrence in the safety matrix of all the systems could be different and thus need to be reconciled into a standardized matrix. The MIL-STD-882 as adopted by DoD should be used as much as possible.

c. **Incorporating Adequate Testing for all Safety Critical Events** - Once the initial table of hazard lists is generated, it is appropriate to begin preparing and formulating the test plan for all safety critical events identified. The main mitigation factor for ensuring safety for COTS/NDI systems is to plan and perform more testing before system fielding and operation.

This thesis identified the current gap as well as the information/data required in system safety assessment for large-scale system integrations, especially in the area of COTS and NDI systems integration. From these required safety-related information/data, and the utilization of system engineering processes and practices, a safety assessment architecture is developed. The Hazard List Table format proposed is a useful tool and provides the necessary information and details necessary whenever required at any phase of the large-scale systems life cycle. As a result, the risk of known hazards is mitigated to as low as reasonably practical (ALARP) and the system health of these large-scale system integrations is improved throughout their life cycles.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The ideal situation for most end users is to be involved in all phases (from development to operational launch) of their systems such that a thorough safety assessment can be performed and the associated hazard risks tracked through the systems' life cycle. With the exception of a handful of technologically-advanced countries with the capability of developing in-house weapon or sensor systems, not many countries have the capacity as well as the technical expertise to realize this situation. The majority of countries have to rely heavily on the defense market (via Foreign Military Sales (FMS) or commercial off-the-shelf (COTS)) to acquire proven systems and then perform some level of adaptation and interface in order to integrate these COTS systems into their combat platforms, such as aircraft or warships, in their bid to build-up a deterrent force.

As a result, the safety assessment for such COTS systems installation aboard various types of combat platforms is usually performed without consideration of overall integration of the system with the major combat platform. In most instances, the safety assessment of the standalone weapon or sensor system will be provided as part of the procurement deliverables to the end users. It is then the responsibility of the system integrator of that particular combat platform to perform the overall safety assessment of the integrated system.

Therefore, this is analogous to having different types of weapon and sensor systems within the large-scale systems integration with their own standalone safety assessment performed. Hence, as the complexity of system integrations increases to achieve certain capability needs, there is an increasing need for system architecture to be developed in order to consolidate the various standalone safety assessments. Then one can identify the overall hazard risks and their corresponding mitigation factors for such large-scale systems integration.

B. OBJECTIVE AND POTENTIAL BENEFITS OF RESEARCH

This research seeks to first identify the information/data required for performing a safety assessment for large-scale systems integration. From these required safety-related information/data, and adopting system engineering processes and practices, a safety assessment architecture can be developed. As a result, the risk of known hazards will be mitigated to as much as possible and the system health of these large-scale system integrations improved throughout their life cycle.

In addition, this research attempts to provide more insight on a holistic analytical and systematic process of performing safety assessment for large-scale systems integrations. This enables the safety-related data to be identified upfront in the system definition phase, progressively traced through the development to implementation phases and finally periodically tracked during the systems' operational cycles.

C. METHODOLOGY AND SYSTEM ARCHITECTURE ADOPTED

1. System Architecture Overview

There are several definitions and research areas with regard to system architecture, most notably from well-known authors in this field. Andrew P. Sage and James E. Armstrong [1] state that architecture is the scheme of arrangements of the components of a system, and that it describes features that are repeated throughout the design and explains the relationship among the system's parts.

Another definition of architecture suggested by Dennis M. Buede [2] includes certain similarities and expansions in detail of the earlier architecture definitions proposed by Sage and Armstrong. Buede further described that an analytical system engineering process begins with an operational concept and includes the development of three separate architectures (functional, physical and operational) as part of this decomposition (Figure 3).

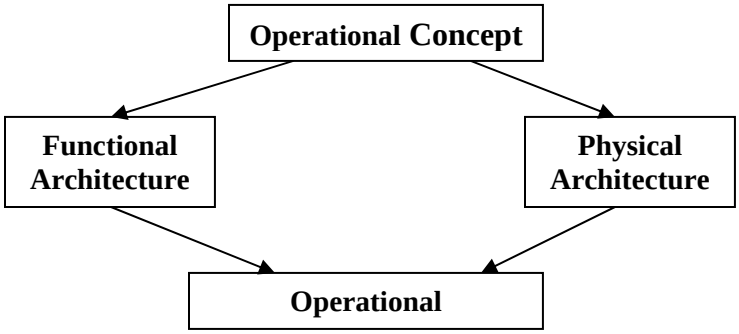


Figure 3. Architecture Development in System Engineering Process

The functional architecture defines what the system must do and the system's functions and the data that flows between the functions. The physical architecture represents the partitioning of physical resources available to perform the system's functions. Finally, the operational architecture is the mapping of functions to resources in a manner that is suitable for discrete-event simulation of the system's functions. In fact, the operational architecture is closely linked to the operational concept (CONOPS), which involves doctrines as well as operating procedures specific to a particular combat platform or even specific to a particular military force structure (i.e., foreign navy, army or air force).

With the various definitions of system architecture proposed above, the fundamental question of when to perform a system safety assessment first requires agreement on what constitutes a 'system'. Only if we can accurately identify the system decomposition, in terms of its functional and physical properties (in addition to its operational concept), can our safety assessment of that system be complete and thorough. Similarly, this concept can be extended to large-scale systems in order to achieve the required capability (i.e., Capability-based System).

The remaining portion of this chapter focuses on the methodology and approach in identifying the architecture needed to perform a detailed system safety assessment for large-scale system integration.

2. Research Methodology

The system design methodology adopted for this research study will be primarily based on the system architecture presented by Dennis M. Buede [2]. Using the three baseline categories, throughout the research study, a case example of Surface-to-Surface (SSM) Missile Weapon System (Harpoon) is adopted to analyze and identify the required information/data for performing a safety assessment of this weapon system to be made operational aboard a warship. An example of a generic SSM system architecture on a warship is described in Figure 4.

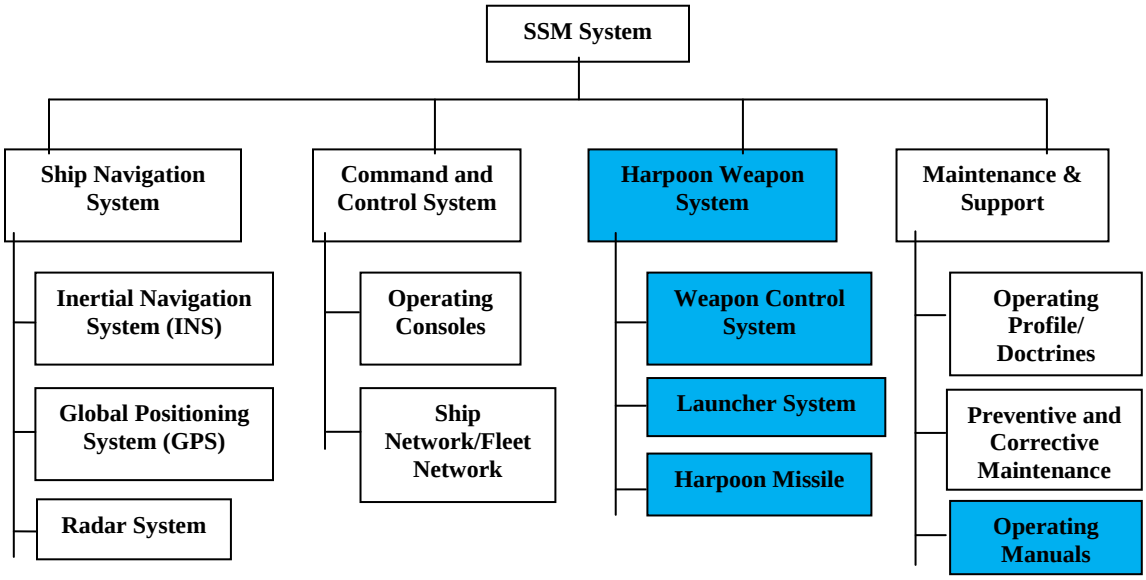


Figure 4. An Example of a Generic SSM System Architecture

Referring to Figure 4, the blocks that are highlighted in blue refer to a standalone system from the Original Equipment Manufacturer (OEM). However, from the standpoint of an end user (i.e., U.S. or foreign Navy), the Harpoon Weapon System is an integral part of the SSM system on her warships (or other combat platforms). As a standalone system, it does not fulfill the required capability of a Surface-to-Surface Missile System if it does not have capable search radar as well as a versatile Command and Control (C2) system that is able to prioritize all surface threats in theater and then designate the necessary engagement orders.

The architecture presented in Figure 4, as well as the brief operational concept described in the previous paragraph, replicates that of a large-scale system integration. In

addition, it shows the distinctly different perspective of a system definition both from an OEM as well as an end user standpoint. This difference in system definition standpoint thus leads the author of this thesis to the different viewpoint of performing a system safety assessment.

From a weapon system OEM viewpoint, their system safety assessment focuses mainly on safety critical faults (i.e., inadvertent launch or misfire/hang-fire situations) that will limit or prevent the system from achieving its capability. There were potentially several assumptions made in OEM safety assessment, which may in turn also indirectly limit their responsibility in ensuring overall system safety installed onto a combat platform. For example, as most C2 systems are uniquely developed by each individual nation, the communication network/interface is not completely made known to the weapon system OEM. Hence, in order to reduce/mitigate the risk of an inadvertent launch, it is essential that the engagement order from C2 is sent correctly and accurately to the weapon system.

Based on the example described above, the immediate question raised will be whose responsibility it is to ensure the engagement order is sent correctly. The weapon system OEM could argue that, for his weapon to operate safely, a correct engagement order has to be received. However, from the standpoint of the end user, the correct engagement order should be checked on both ends (i.e., as sent out by the C2 system and received by the weapon system). Depending on the level and depth of interface that the weapon system has with the C2 system, this argument of whose responsibility it is to ensure the integrity of critical messages/orders from one party to another will continue. To some extent, it may affect the successful conduct of a system safety assessment in its entirety.

3. Research Focus Areas

Considering the above brief description of one typical system integration problem, and based on the proposed system architecture described by Buede in Figure 3, the safety assessment architecture for large-scale system integration can be broadly broken down into the following main areas/topics to be researched in detail:

a. Design considerations, development and qualification test results/data, past track records, safety program adopted, safety requirements identification and allocation, hazard/risk analysis and design verification process (i.e., functional safety)

b. Safety to as well as between interfacing platforms, safety to personnel handling the weapon system (i.e., physical safety)

c. Weapon Safety template, Fleet doctrines and operating procedures, preventive and corrective maintenance schedule (i.e., operational safety)

The general SSM architecture shown in Figure 4 and the example of interfacing a Harpoon Weapon System on a navy platform will be referenced again in the following chapters to explain certain key points, as well as to highlight certain proposed improvements on where system safety assessment could be implemented.

Finally, from the information/data gathered in the above areas of research, a template for hazard/risk analysis could be developed for traceability. In addition, the key areas in the SE process will also be identified such that these safety-related information/tasks could be systematically obtained, gathered and maintained through the systems' life cycle.

II. OVERVIEW OF SYSTEM SAFETY ASSESSMENT

A. SYSTEM SAFETY IN DEFENSE INDUSTRY

1. Emergence of System Safety Program

System safety itself arose out of ballistic missile programs in the 1950s [5], when the Atlas and Titan ICBMs were being developed; intense political pressure was focused on building a nuclear warhead with delivery capability as a deterrent to nuclear war. In these first missile system projects, system safety was not identified and assigned as a specific responsibility. Instead, as was usual at the time, each designer, manager, and engineer was assigned responsibility for safety. These projects, however, involved advanced technology and much greater complexity than had previously been attempted, and the drawbacks of the standard approach to safety became clear when many interface problems went unnoticed until it was too late.

Within 18 months after the fleet of 71 Atlas F missiles became operational, four blew up in their silos during operational testing. The missiles also had an extremely low launch success rate. Not only were the losses themselves costly, but the resulting investigations detected serious safety deficiencies in the system that would require extensive modifications to correct. In fact, the cost of the modifications would have been so high that a decision was made to retire the entire weapon system and accelerate deployment of the Minuteman missile system [3].

When the early aerospace accidents were investigated, it became apparent that the causes of a large percentage of them could be traced to deficiencies in design, operations, and management. The previous “fly–fix–fly” approach was clearly not adequate. In this approach, investigations were conducted to reconstruct the causes of accidents, action was taken to prevent or minimize the recurrence of accidents with the same cause, and eventually these preventive actions were incorporated into standards, codes of practice, and regulations. Although the fly–fix–fly approach was effective in reducing the repetition of accidents with identical causes, it became clear to the Department of Defense (DoD), and later to others, that it was too costly and, in the case of nuclear

weapons, unacceptable to prevent accidents only after they occur a first time. This realization led to the adoption of system safety approaches to try to prevent accidents before they happen.

The first military specification on system safety was published by the U.S. Air Force (Ballistic Systems Division) in 1962, and the Minuteman ICBM became the first weapon system to have a contractual, formal, disciplined system safety program. From that time on, system safety received increasing attention, especially in Air Force missile programs where testing was limited and accident consequences were serious. The U.S. Army soon adopted system safety programs because of the many personnel it was losing in helicopter accidents, and the U.S. Navy followed suit. In 1966, the DoD issued a single directive requiring system safety programs on all development or modification contracts.

At first, there were few techniques that could be used on these complex defense systems. But, step by step, the specialized safety engineering and operational safety practices that had evolved over the years were integrated with scientific, technical, and management techniques that were newly developed or adapted from other activities. Particular emphasis was placed on hazard analysis techniques, such as fault trees, which were first developed to cope with complex programs such as Minuteman.

2. Definition of System Safety

System safety uses systems theory and system engineering approaches to prevent foreseeable accidents and to minimize the results of unforeseen ones. Losses in general, not just human death or injury are considered. Such losses may include destruction of property, loss of mission, and environmental harm. The primary concern of system safety is the management of hazards: their identification, evaluation, elimination, and control through analysis, design and management procedures. Mueller, in 1968, described the then new discipline of system safety engineering as “organized common sense” [4].

System safety is a planned, disciplined, and systematic approach to identifying, analyzing, and controlling hazards throughout the life cycle of a system (Figure 5 shows the system life cycle model as defined in DoD 5000) in order to prevent or reduce accidents. System safety activities start in the earliest concept development stages of a

project and continue through design, production, testing, operational use, and disposal. One aspect that distinguishes system safety from other approaches to safety is its primary emphasis on the early identification and classification of hazards so that corrective action can be taken to eliminate or minimize those hazards before final design decisions are made.

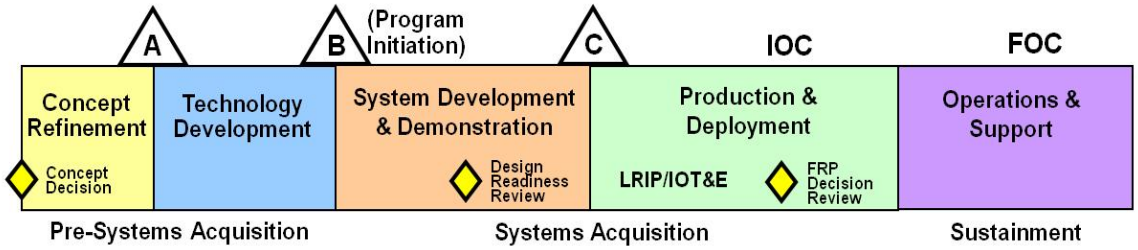


Figure 5. DoD System Life Cycle Model (From: [21])

System safety is more than just system engineering. Essentially, system safety engineering is an important part of system safety, but the concerns of system safety extend beyond the traditional boundaries of engineering. In 1968, Jerome Lederer, then the director of the NASA Manned Flight Safety Program for Apollo wrote [5]:

> System safety covers the total spectrum of risk management. It goes *beyond the hardware* and associated procedures of system safety engineering. It involves attitudes and motivation of designers and production people, employee/management rapport, the relation of industrial associations among themselves and with government, human factors in supervision and quality control, documentation on the interfaces of industrial and public safety with design and operations, the interest and attitudes of top management, the effects of the legal system on accident investigations and exchange of information, the certification of critical workers, political considerations, resources, public sentiment and many other non-technical but vital influences on the attainment of an acceptable level of risk control. These nontechnical aspects of system safety cannot be ignored.

Using these general principles, system safety attempts to manage hazards through analysis, design, and management procedures. Key activities include top-down system hazard analyses (starting in the early concept design stage to eliminate or control hazards and continuing during the life of the system to evaluate changes in the system or the environment), documenting and tracking hazards and their resolution (establishing audit

trails); designing to eliminate or control hazards and minimize damage, maintaining safety information systems and documentation; and establishing reporting and information channels.

System Safety is a continuing effort and ever-increasing important task in all weapon systems acquisition. While it is seen as a near impossible task to achieve zero accidents/mishaps, the ultimate aim is to strive for reduction/mitigation of risks to as low as reasonably practical (ALARP). As quoted by Jerome Lederer earlier, System Safety is a culture that needs to be well understood and supported, especially by higher management. A similar memorandum sent out by the Secretary of Defense in 2003, stating that, "I challenge all of you to reduce the number of mishaps and accident rates by at least 50% in the next 2 years," [15] clearly demonstrated the strong desire and paramount importance of ensuring effective and safe fighting forces. Subsequently, through the dissemination of this memorandum, the DoD Oversight Council (DSOC) was established by the Under Secretary of Defense for Personnel and Readiness [16] to provide governance of accident reduction efforts.

3. System Safety Standards

The first system safety assessment standard, MIL-STD-882, was issued in June 1969 and a system safety program became mandatory on all DoD-procured products and systems. The first revision (MIL-STD-882A) was made in June 1977, focusing on the concept of risk acceptance as a criterion for system safety programs. The hazard probability and established categories for frequency of occurrence to accommodate the long-standing hazard severity categories was also introduced. Next, MIL-STD-882B, revised in March 1984, continued the evolution of detailed guidance in both engineering and management requirement, with more emphasis on facilities and off-the-shelf acquisition, while software was addressed in some detail for the first time. About three years later, the expanded software tasks and the scope of the treatment of software by system safety was included in this revision.

In Jan 1993, the MIL-STD-882C revision included the integration of hazard and software system safety efforts and removed the individual software tasks in the earlier

revision. As a result, the safety analysis would identify the hardware and software tasks together in a system. Under the Military Specifications and Standards Report (MSSR) initiative, MIL-STD-882D was considered important to continue, as long as it was converted to a performance-based standard practice *what you want vs. how to do it*. In this Feb 2000 revision [6], task descriptions were also removed. In summary, the MIL-STD-882 describes eight mandatory system safety steps as follow:

1. Document the system safety approach
2. Identify ESOH hazards
3. Assess the risk
4. Identify risk mitigation measures
5. Reduce risk to an acceptable level
6. Verify risk reduction
7. Review hazards and accept risk by appropriate authority
8. Track ESOH hazards, their resolution, and residual risk throughout the system lifecycle

Mishap severity categories are defined to provide a qualitative measure of the most reasonable credible mishap resulting from personnel error, environmental conditions, design inadequacies, procedural deficiencies, or system, subsystem, or component failure or malfunction. Suggested mishap severity categories are shown in Table 1. The dollar values shown in this table should be established on a system-by-system basis depending on the size of the system being considered to reflect the level of concern.

Table 1. Suggested Mishap Severity Categories

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding $1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding $200K but less than $1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding $10K but less than $200K, or mitigatible environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding $2K but less than $10K, or minimal environmental damage not violating law or regulation.

Mishap probability is the probability that a mishap will occur during the planned life expectancy of the system. It can be described in terms of potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative mishap probability to a potential design or procedural hazard is generally not possible early in the design process. At that stage, a qualitative mishap probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a mishap probability is documented in hazard analysis reports. Suggested qualitative mishap probability levels are shown in Table 2.

Table 2. Suggested Mishap Probability Levels

Description	Level	Specific Individual Item	Fleet or Inventory
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in that life.	Unlikely, but can reasonably be expected to occur
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible

The **Mishap Risk Assessment matrix** is a classification by mishap severity and mishap probability to be performed. This assessment allows one to assign a mishap risk assessment value to a hazard based on its mishap severity and its mishap probability. This value is often used to rank different hazards as to their associated mishap risks. Table 3 shows an example of this Risk Assessment matrix as derived from MIL-STD-882D.

Table 3. Mishap Risk Assessment Values

Frequency of Occurrence	Severity			
	Catastrophic	Critical	Marginal	Negligible
Frequent	1	3	7	13
Probable	2	5	9	16
Occasional	4	6	11	18
Remote	8	10	14	19
Improbable	12	15	17	20

Mishap risk assessment values are often used in grouping individual hazards into mishap risk categories. Mishap risk categories are then used to generate specific action such as mandatory reporting of certain hazards to management for action or formal acceptance of the associated mishap risk. Table 4 shows an example listing of mishap risk categories and the associated assessment values. In the example, the system management has determined that mishap risk assessment values 1 through 5 constitute "High" risk while values 6 through 9 constitute "Serious" risk.

Table 4. Mishap Risk Categories and Mishap Risk Acceptance Level

Mishap Risk Assessment Value	Mishap Risk Category	Mishap Risk Acceptance Level
1 – 5	High	Component Acquisition Executive
6 – 9	Serious	Program Executive Officer
10 – 17	Medium	Program Manager
18 – 20	Low	As directed

B. IMPLEMENTATION OF SAFETY ASSESSMENT MATRIX

1. Overview of Harpoon Weapon System

In 1965, the U.S. Navy began studies for a missile in the 45 km (25 nm) range class for use against surfaced submarines. The name *Harpoon* was assigned to the project (i.e., a harpoon to kill "whales," a naval slang term for submarines). After the sinking of the Israeli destroyer *Eilat* in 1967 by Soviet-built anti-ship missiles, the U.S. Navy saw the need to develop a dedicated anti-shipping missile, and therefore *Harpoon*'s primary mission became surface ship attack. The development project was formally begun in 1968, and the missile designator **ZAGM-84A** was allocated in 1970 after the Navy had issued a formal RFP (Request For Proposals). In June 1971, McDonnell Douglas was awarded the prime contract for *Harpoon*, and the first test missile flew in October 1972.

By that time it had already been decided to develop air-launched, ship-launched and submarine-launched *Harpoon* variants, designated **AGM-84A**, **RGM-84A** and **UGM-84A**, respectively. Because the range requirement was increased to 90 km (50

nm), turbojet propulsion was selected by McDonnell Douglas. Production of the *Harpoon* began in 1975, and the first version to enter service was the shipborne RGM-84A in 1977, followed by the AGM-84A on P-3 aircraft in 1979. The UGM-84A became operational on attack submarines in 1981. The AN/SWG-1(V) Harpoon Ship Command Launch Control System (HSCLCS) is the element of the surface ship weapon system that prepares and launches the Harpoon cruise missile.

The *Harpoon* is the only dedicated anti-ship missile in service with U.S. armed forces. In recent years, it has been developed into several advanced versions/variants (i.e. Block 1C, 1G and II), including the *SLAM* (Stand-off Land Attack Missile) derivatives for high-precision attacks on land targets. Notwithstanding, its weapon system has also been upgraded (to Advanced Harpoon Weapon Control System) to handle more sophisticated and complex network-centric integration. The *Harpoon*/*SLAM* will remain in service with the U.S. Navy for the foreseeable future and it remains the world's most successful anti-ship missile, featuring autonomous, all-weather, over-the-horizon capability. As of 2008 (according to the Boeing website), more than 7,200 Harpoons have been produced, with about twenty-nine countries as Harpoon customers.[1]

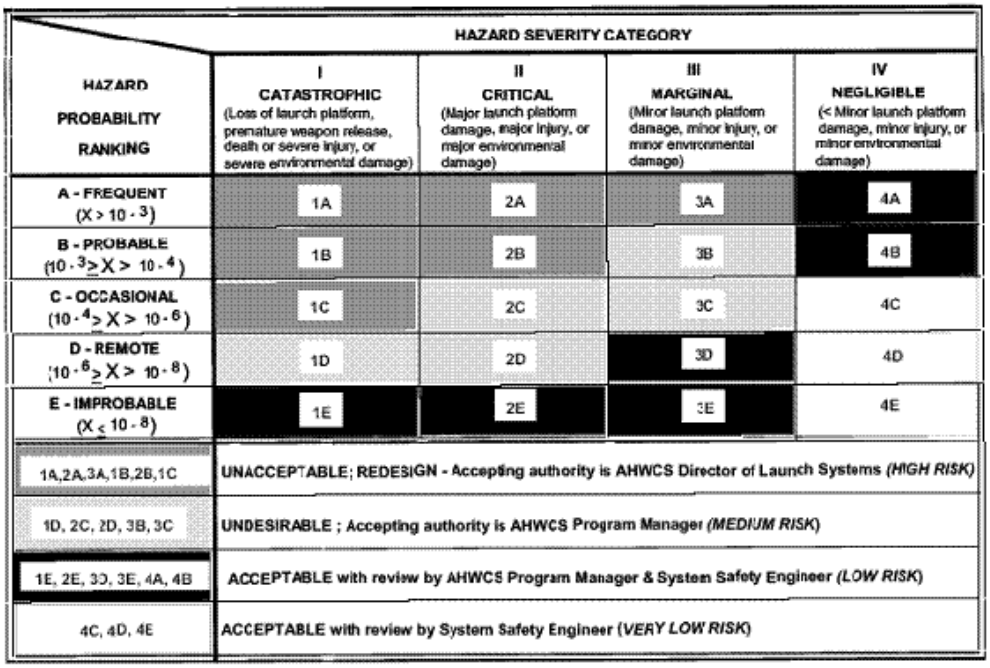
Throughout the development of the Harpoon missile and its weapon control system, McDonnell Douglas (a wholly-owned subsidiary of The Boeing Company) had maintained a consistent safety oversight program to ensure that all safety aspects of this weapon were addressed, monitored and mitigated. Figure 7 (page 17) shows the hazard risk matrix that was used in their classification of hazard risk depending on its probability of occurrence; the corresponding acceptance level of risk is also clearly identified.

1 Harpoon Missiles can only be acquired via Foreign Military Sales (FMS), while its control system (HSCLCS or AHWCS) can be acquired either FMS or commercially through McDonnell Douglas, a wholly-owned subsidiary of The Boeing Company.

Figure 6. Harpoon Weapon on Different Combat Platforms (From: [22])

The most important point to note in Figure 7 is that, while the hazard severity category can be adapted to other foreign armed forces, the hazard probability ranking presented is believed to be based on a certain USN platform as well as its associated operational profile. This is evident as Boeing and McDonnell Douglas were the prime contractor during the 1970s for the USN in developing the first generation of Harpoon missile and weapon control system. After the first operational deployment of Harpoon, a full safety assessment was not performed for each subsequent variant and upgrade of the system (i.e., assessments only addressed the areas where the upgrades were performed).

As the Harpoon missile and its weapon control system established a proven track record, it was extended to more deployments in various combat platforms. However, the same safety matrix in Figure 7 is being adopted for other combat platform installations. Similarly, though Harpoon was made available to interested allied countries of the U.S., most of these foreign armed forces did not have access to the overall safety assessment performed (i.e., in most cases, the information is classified and non-releasable).



HAZARD PROBABILITY RANKING	HAZARD SEVERITY CATEGORY I CATASTROPHIC (Loss of launch platform, premature weapon release, death or severe injury, or severe environmental damage)	II CRITICAL (Major launch platform damage, major injury, or major environmental damage)	III MARGINAL (Minor launch platform damage, minor injury, or minor environmental damage)	IV NEGLIGIBLE (< Minor launch platform damage, minor injury, or minor environmental damage)
A - FREQUENT ($X > 10^{-3}$)	1A	2A	3A	4A
B - PROBABLE ($10^{-3} \geq X > 10^{-4}$)	1B	2B	3B	4B
C - OCCASIONAL ($10^{-4} \geq X > 10^{-6}$)	1C	2C	3C	4C
D - REMOTE ($10^{-6} \geq X > 10^{-8}$)	1D	2D	3D	4D
E - IMPROBABLE ($X \leq 10^{-8}$)	1E	2E	3E	4E

1A,2A,3A,1B,2B,1C	UNACCEPTABLE; REDESIGN - Accepting authority is AHWCS Director of Launch Systems *(HIGH RISK)*
1D, 2C, 2D, 3B, 3C	UNDESIRABLE ; Accepting authority is AHWCS Program Manager *(MEDIUM RISK)*
1E, 2E, 3D, 3E, 4A, 4B	ACCEPTABLE with review by AHWCS Program Manager & System Safety Engineer *(LOW RISK)*
4C, 4D, 4E	ACCEPTABLE with review by System Safety Engineer (*VERY LOW RISK*)

Figure 7. Safety Assessment Matrix Adopted by The Boeing Company (From: [23])

In this section, an illustration of the development of the Harpoon and its weapon control system provided some indication of the complexity of safety assessment to be addressed for future large-scale system integrations development. Most armed forces, probably including U.S. and other technology-advanced countries, would potentially require information on safety assessment of various sub-systems (either developed in-house or operated by different agencies) of large integrated systems (in different combat platforms). As such, system safety assessment of current platform-based approach may not be feasible in a capability-based network-centric system required to address the ever-growing complexity of threats in theater.

C. CURRENT GAPS IN SAFETY ASSESSMENT PERFORMED

The following shows some current gaps identified for conducting safety assessment for large-scale system integrations:

a. Most end users (i.e., foreign armed forces), who do not have the capacity and technology to develop their own weapon systems, could only obtain safety assessments performed for a standalone weapon system and hence are not able to address the overall safety assessment of an integrated system in order to achieve their needed capability.

b. As the complexity of system integrations increases, or the development of large-scale systems integration, changes or upgrades being done in one system will affect the overall system safety and hence there will be a need to review the entire system safety assessment. There is currently no identified process that could allow tracking and monitoring of all changes in large-scale system integrations.

c. The rapid and more organized threat emergence in recent years has led to the constant review of each nation's concept of operations (CONOPS) as well as doctrines. These operational changes directly affect how systems are to be operated, the operational profiles, which in turn leads to the changes in the probability of hazard occurrence and their associated consequences.

III. SAFETY ASSESSMENT REQUIREMENT FOR LARGE-SCALE SYSTEMS INTEGRATION

A. SYSTEM SAFETY CHALLENGES FOR NDI/COTS

As concluded in Chapter II, one of the current gaps in safety assessment for large-scale system integrations was the inability to address the overall safety assessment of an integrated system in order to achieve their needed capability. From the prospective of foreign armed forces, one possible reason for this gap in safety assessment is due to NDI/COTS purchases from established weapon system contractors and/or via government-agency (i.e., FMS buy). This can be further illustrated using Figure 8 with respect to the DoD 5000.2 system life cycle process model (recently updated in 2009), where NDI/COTS procurement probably occurs at milestone B.

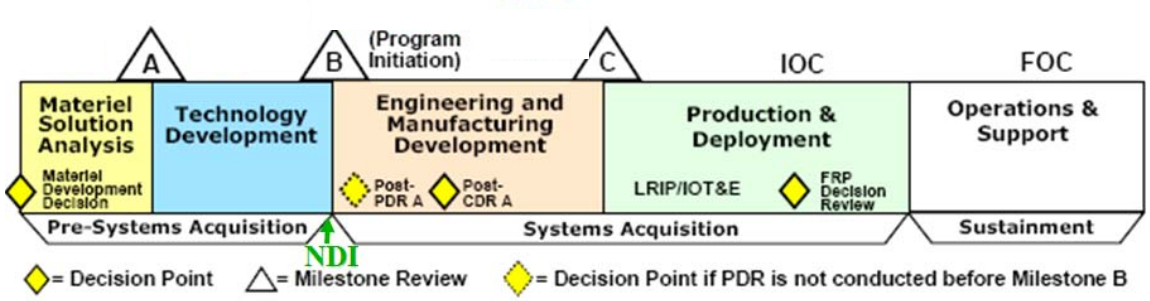


Figure 8. DoD 5000.2 (2009) System Life Cycle Process Model (From: [21])

Commercial off-the-shelf (COTS) is the term most often used to refer to commercial items already developed and readily available for purchase by the government. The definition of Non-Developmental Item (NDI) follows a similar definition to that of COTS. The main benefits of NDI/COTS acquisition include savings on research and development costs and reduced the risk associated with new development. On the other hand, NDI/COTS also posed other challenges and pitfalls such as limited changes to the basic design and changes not controlled by the end user (i.e., OEM has the overall configuration control). Lastly, NDI/COTS also limits the end user in obtaining information about the developmental phases of that product and hence may not

allow full awareness of the problems identified and methodology to resolve them; safety-related identification and mitigation process is one type of information termed "non-releasable" in NDI/COTS acquisition.

With reference to the case example of procuring a Harpoon Weapon System used for this thesis research, most if not all foreign armed forces obtained their weapon systems at milestone B (refer to Figure 8) or beyond. This essentially means that about one-third of the system safety information resides with the original equipment manufacturer (OEM) or most of the time this information is non-releasable due to classification restriction (i.e., security and economics aspects). Other potential problems faced when obtaining these NDI/COTS include the following:

- Performance specifications represent developing country's needs, threats, and operational environment vis-à-vis the buyers'
- NDI-COTS System may be designed for different tactics, doctrine and logistic support structure (skewed toward the developing country)
- Usually designed for different user training, skill levels, strength, culture, and combat environment (i.e., human factors, symbology used in man-machine interface (MMI), anthropometric requirements, etc.)
- Not specifically designed for interoperability or compatibility with user systems.
- System modifications to meet user threats may be difficult and economically not feasible (i.e., re-design the whole system)

In consideration of the above challenges and difficulties faced by most NDI/COTS users, it is evident that the testing and evaluation of these NDI/COTS components before they are installed for field use becomes of paramount importance. The following section will describe in detail the need for operational testing and evaluation in NDI/COTS procurement.

B. IMPORTANCE OF TESTING AND EVALUATION IN SYSTEM SAFETY PROCESS

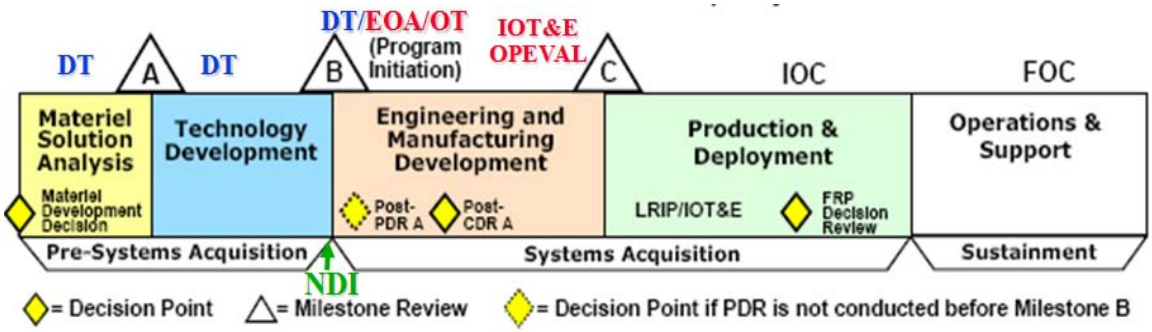
With reference to the DoD 5000.2 process presented in the section above, the pre-system acquisition phase can be described as the developmental testing and evaluation (DT & E) of the system. This is the initial system concept design phase and probably the 'root' of all subsequent system safety issues of the life cycle downstream. In fact, all

safety-related design considerations and safety interlocks were determined here based on certain operational concepts and doctrines/policies put in place by the developing country. In addition, this DT & E phase is beyond the control of the NDI/COTS user and will have limited safety information associated with it. Therefore, this emphasizes the importance of focusing testing and evaluation at the start of milestone C, as shown in Figure 8, for NDI/COTS users as an alternate approach to verifying the critical safety design features of the system.

The difference between DT & E and Operational Test & Evaluation (OT & E) lies in the scope of tests conducted in their respective phases. In DT & E, tests are in a controlled and repeatable environment, and the main objective of such tests is to demonstrate that the system performs as planned at each stage of the development and thus meets the intended system specifications (for example, Harpoon Weapon System Specifications [22]). On the other hand, OT & E focuses on evaluating a system's operational effectiveness and suitability in accordance with end user doctrine and operating procedures. In this aspect, this phase is the most crucial phase for the end user to determine the robustness of the NDI/COTS in realistic operational environment (for example, Harpoon Weapon System Specifications [22]). Therefore, it is also in this phase where further system safety-related problems will be discovered (i.e., due to integration of several NDI/COTS components).

As shown in Figure 9, three main domains contribute to the eventual goal of attaining combat effectiveness in any large-scale systems integration acquisition, namely Personnel & Training, Tactics & Doctrine, and Weapon Technical Performance. In relation to the test and evaluation phases, Weapon Technical Performance will be validated in the DT & E phase, which is the responsibility of the OEM. Both the Personnel & Training and Tactics & Doctrine will be validated through the OT & E phase, which is within the control of the end user. As clearly illustrated in Figure 9, each of the three domains has to interact with the others in order to achieve the final objective as indicated in the center overlapping the three domains. For example, a certain level of tactical training of the operators needs to be conducted in accordance with the specified tactics and doctrine developed by the end user. In addition, modeling and simulation

(M&S), such as the Army's Janus combat simulation, could be incorporated to further evaluate if the weapon system functions as intended in accordance with the desired tactics required by the user. Finally, the human factors as well as safety to operating personnel must be demonstrated so that the weapon system may be deemed 'fit for use.'



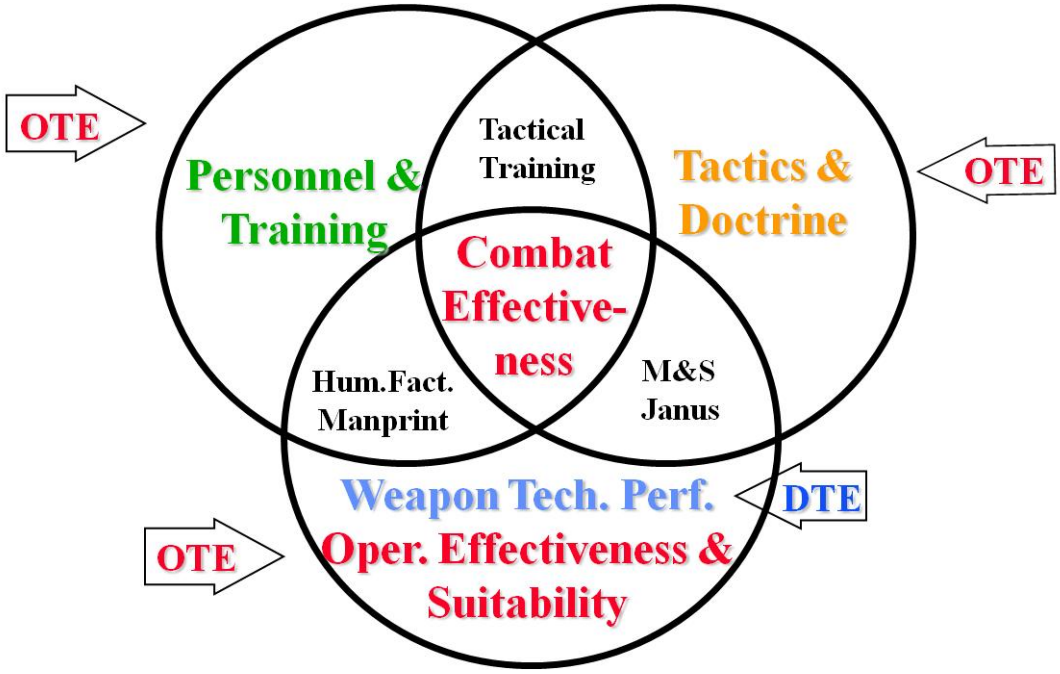


Figure 9. Combat Effectiveness In Relation To DT & E and OT & E (From: [21])

From another point of view, it can also be seen that as the system evolves through the various life cycle stages, more and more errors/problems surface, as shown in Figure 10. During the requirement definition phase, requirement errors first develop that could be due to uncertainty in the concept of operations and usage of the system. As the system evolves into the design phase, these requirement errors are then compounded with

inherent design errors. Subsequently, in the implementation phase, these design errors may lead to hardware and software errors, in addition to the errors created in the earlier two phases. Finally, as the system reaches the testing phase, the effects of uncontrolled errors, such as environment conditions and random operator handling errors will become more significant and could make it even harder to trace and determine the source of error. This leads to the decision to focus on the OT & E phase as one of the mitigating factors in overcoming the current gap of system safety for large-scale integration.

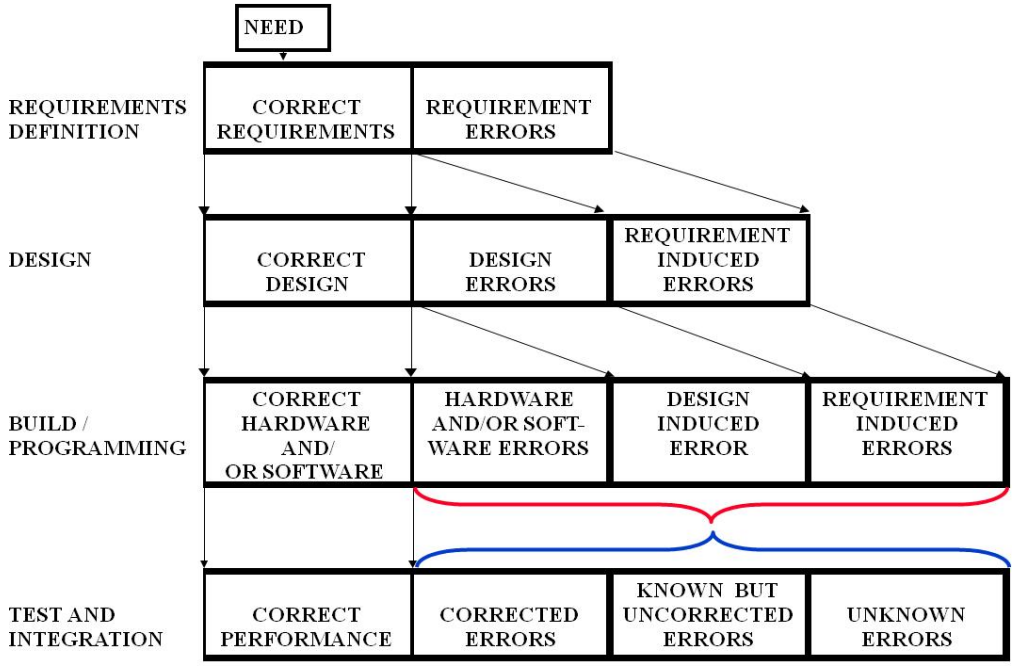


Figure 10. Errors Increases As the System Goes Through the Life Cycle (From: [21])

C. SYSTEM LIFE CYCLE PROCESS MODEL FOR NDI/COTS

As highlighted in the earlier section on the potential problems with regard to system safety faced by NDI/COTS, Figure 11 briefly shows a typical system life cycle process model of a NDI/COTS system. This is analogous to a large-scale systems integration, whereby concept of operations as well as systems requirement formulation are the critical parameters in this front end planning phase. The key difference here in comparison with the DoD System Life Cycle Process model (shown in Figure 8) can be explained using the case example of the Harpoon Weapon System.

As briefly described in Chapter II, the Harpoon Weapon System was developed to counter a threat identified by the U.S. Navy in 1965; hence, this defined the concept of operation for the Harpoon Weapon System. In today's context, from the perspective of a current FMS customer, the concept of operation for a Surface-to-Surface Weapon System during the front end planning phase is likely to be different than the U.S. Navy Harpoon CONOPS. The Harpoon Weapon System may be just one of the many potential systems available on the market to be considered as part of the customer's overall CONOPS during the front end planning phase.

As the FMS customer becomes clearer on her concept of operations, the required systems to meet her needs will then be defined, which will lead into the next phase known as systems acquisition management. Depending on the nature and organizational structure of the FMS customers, their required systems may be procured under a main contract or be broken down into several sub-systems' contracts. Again, this is similar to the process of large-scale systems integration procurement.

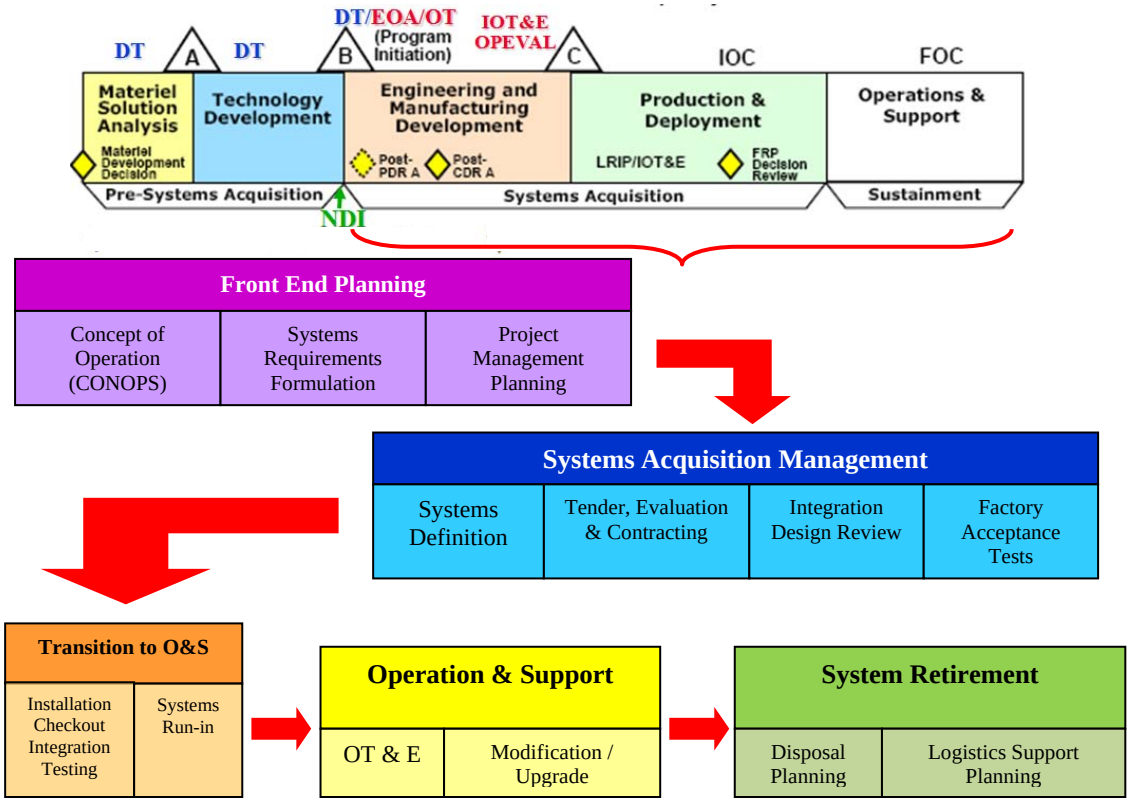


Figure 11. System Life Cycle Process Model for NDI/COTS (After: [21])

It is becoming more and more complex (for a single contractor) as well as economically not feasible to have a large enough budget and time to achieve the full operational capability of a large-scale systems integration. As such, systems are procured and then made operational in phases before they are finally put together to achieve the integrated operational capability desired. Similarly, this process flow of a large-scale systems integration life cycle fits in perfectly to the process model as shown in Figure 11.

D. IMPORTANCE OF A SYSTEM INTEGRATOR (SI) AND INTEGRATED PROGRAM MANAGEMENT TEAM (IPMT)

It is without doubt that the successful implementations of a large-scale systems integration requires not just various subject matter experts (SMEs), but also an overall System Integrator (SI) serving as the first important piece of the puzzle to a successful overall safety assessment. The role of the SI can be defined as follow:

a. Understand the overall CONOPS required and the role each system plays in a large-scale systems integration
b. Meet the intended IOC/FOC milestones for the overall large-scale systems integration in consideration of the various sub-systems' contracts and their respective schedules
c. Serve as possible interfacing link between the end user, various contractors and SMEs
d. Resolve critical integration issues throughout the life cycle process
e. Provide timely update on progress to management and end user

As described above, the role and responsibility of the SI is enormous; it requires not a single person but a dedicated team that can cover the various aspects of the large-scale systems integration problems. This leads to the second recommendation of forming an IPMT, which comprises mainly the different systems to be procured within the large-scale systems integration. This approach will help in breaking down the more complex higher-level problems into various sub-areas whereby interface/integrating issues can be localized and resolved completely. Regular integration reviews, led by the SI, should be conducted to keep track of all problems, be they solved or outstanding. This is essential in the subsequent formulation of the overall system safety assessment.

Last but not least, the end user should also be engaged early during the system acquisition management phase. In fact, it is important to obtain end-user input on the

eventual OT & E requirements such as scenarios, specific aspects of the integration to be demonstrated, etc, and then lay out the plan leading up to the final objective. A working group composed of the end user, the SI and the various sub-system managers is recommended during this phase of the system life cycle, so that all interface/integration issues, progress updates on the various systems and any potential technical/schedule/cost risks are foreseen. Nonetheless, the overall system safety assessment should also begin in this phase and be addressed in the working group meeting.

E. SYSTEM SAFETY REQUIREMENT FOCUS

The system life cycle process model for a large-scale systems integration shown in Figure 11 defines the 'backbone' of the system safety architecture, which allows the author of this thesis to gather the essential and necessary information required for the analysis downstream. As highlighted earlier in this chapter, about one-third of the system safety information resides with the original equipment manufacturer (OEM); this is clearly shown in the discussion on the differences between the system life cycle adopted by DoD and the proposed system life cycle process model for a large-scale systems integration (Figure 11). The system safety assessment of large-scale systems integration can be broken into the following area of focus during its life cycle:

- Safety to Interfacing Platform – This aspect looks into issues such as qualification tests conducted vis-à-vis interfacing platform structures, EMI/EMC issues, maintenance-related safety issues, etc.
- Safety to Personnel and Operator Handling the System – This aspects looks into the Human-System Interface (HSI) in terms of operator risk and exposure to ordnance
- Safety Template Optimization – This focuses on the safety range of weapon damage boundaries, ordnance and Electromagnetic and Energetic Devices (EEDs)

In the following chapters, the methodology and evaluation criteria for the three areas of focus above will be described in detail.

IV. SYSTEM-OF-SYSTEM SAFETY METRICS

A. NEED FOR JOINT SAFETY METRICS

The complex nature of today's war-fighting operations has led to the emergence of the large-scale systems integration; similarly for system safety, especially in critical areas such as weapon systems, there is an increasing need to formulate an integrated system safety assessment. This is the reason the Defense Safety Oversight Council (DSOC) Acquisition and Technology Programs Task Force (ATP TF), on 21 July 2005, approved a proposal to streamline the weapon safety review process and chartered a Joint Weapon Safety Working Group to develop and refine a collaborative, defense-wide process for USSOCOM (United States Special Operations Command) support. As shown in Figure 12, weapon safety review board certifications in support of USSOCOM acquisition programs historically were obtained through multiple reviews by the respective system safety boards and organizations in each of the departments [7].

Figure 12. List of Safety Review Boards between the various Services in DoD (From: [7])

The process to certify systems as safe for use by members of more than one Service has been to conduct individual Service system safety reviews by each of the Services whose members would be expected to employ those systems. While each individual Service has long-standing weapon safety review processes designed to meet their Service-unique requirements, multiple individual system safety reviews conducted in series by each Military Department and/or Service for a particular joint weapon or weapon system are expensive, time consuming and redundant. In addition, a multiple review board approach has the potential for conflicting safety requirements and recommendations resulting in inconsistent safety designs and/or operating procedures.

Therefore, it is both prudent and logical to require that a single, integrated and consolidated weapon safety review and certification be conducted for each USSOCOM system in a coherent, collaborative manner by the respective weapon safety review authorities. Hence, weapon safety representatives from USSOCOM, the Army, Navy, Marine Corps, Air Force, Department of Defense Explosives Safety Board (DDESB), and Office of the Under Secretary of Defense (OUSD) for Acquisition Technology & Logistics (AT&L) coordinated the development of a Joint process that addresses Joint safety release and certification. This process eliminates the inefficiencies inherent in the existing individual Military Department and Service system safety review processes when examining, for safety purposes, any USSOCOM weapon system with Joint application. As a result, this Joint collaborative review process accelerates the fielding of weapon systems to the USSOCOM war-fighter without compromising safety.

B. PROPOSED SAFETY METRICS

The Defense Safety Oversight Council (DSOC) Acquisition and Technology Programs (ATP) Task Force funded development of the System Safety Metrics Method in 2006 [10], which aims to develop a model to serve as a useful tool to gauge the health of a safety program at any stage of the lifecycle of the program. The proposed System Safety Metrics Method consists of a recommended scale (0-5), 39 inquiry items, detailed data collection sheets, and a means to track the data. Figure 13 shows a recommended approach in evaluating the system safety program effectiveness.

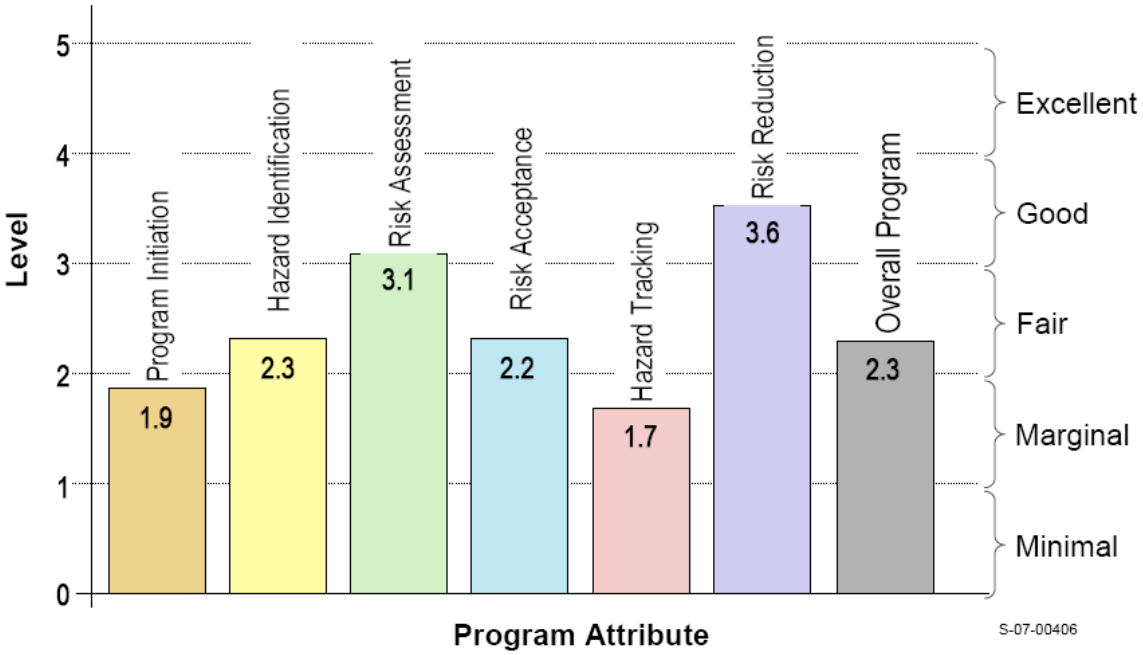


Figure 13. Proposed System Safety Metrics (From: [10])

The System Safety Metrics Method depicted above consists of:

- Data Gathering Criteria
- Scale
- Table of Inquiry Items
- Composite Index of Inquiry Items
- Results Database (Microsoft Excel spreadsheet)

As mentioned above, the purpose of the System Safety Metrics Method is to gauge the efficacy of a system safety program. To accomplish this, interviews are conducted with program practitioners. Answers to standardized interview questions provide data that are then used to profile the program. Workshop participants were a group of more than forty System Safety specialists from around the U.S. and abroad, including agencies such as DoD, NASA, the European Space Agency, several universities, and the FAA. The results gathered from the workshop identified three primary categories of measure as an effective paradigm: people, tools, and procedures/methods.

A draft matrix of questions then captures a set of metrics pointing toward excellence. Finally, the draft set of about more than 140 questions can be used to gather information about the current state of a system safety program or organization. As described in the earlier paragraph, this system safety metrics method focuses on the overall safety program adequacy while diminishing the importance of detailed analysis and traceability of safety hazards associated with the system.

In addition, this method would truly benefit a development program whereby a safety program needs to be in place at the beginning of the life cycle, as shown in DoD 5000.2 (2009) System Life Cycle Process Model. It may be less effective in assessing the system safety for COTS/NDI systems integration, which requires gathering and consolidating different system safety models and matrices generated from differing safety program adopted by various OEMs.

C. SYSTEM SAFETY ASSESSMENT FUNCTIONAL HIERARCHY

In order to formulate an integrated system safety assessment, it is important to first describe the essential functions that are required to fulfill this objective. Through gap analysis and information gathered in this thesis research, Figure 14 depicts the proposed four main functions critical to a large-scale systems integration safety assessment, namely Identify, Mitigate, Create Traceability and Gain Acceptance. The details of each function are described as follows:

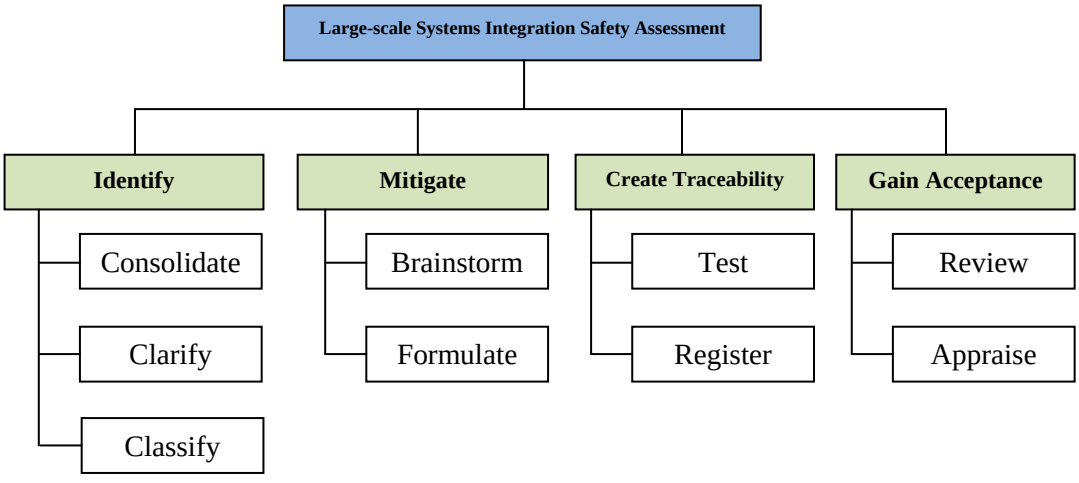


Figure 14. System Safety Assessment Functional Hierarchy

Identify – The first function of system safety assessment is to have the ability to consolidate, clarify and classify all risks and hazards within the large-scale systems integration. This is the phase where much of the data collection and consolidation of different system safety reports from the various sub-systems within the large-scale systems integration architecture is conducted. Next, clarification with each sub-system's OEM on their safety report and basis of their safety hazards should be conducted so that the team will be able to understand the assumptions taken in deriving the residual risks.

With these clarifications, further classification of the risks could be performed so as to tailor the nature and complexity of the integration required as well as the concept of operations desired; these could potentially result in new risks or hazards being identified. This first function of system safety assessment is considered to be the most important and critical portion in the safety assessment hierarchy. The level of details and adequacy of mitigation factors that follow heavily depends on the amount of safety-related information and their associated supporting documents and references gathered from the individual COTS/NDI OEMs.

Mitigate – With the identification and clarification of the list of hazards associated with the large-scale systems integration conducted in the earlier function, it is then the task of this function to brainstorm and formulate all possible mitigation factors in order to reduce these hazards to "as low as practically reasonable." This function is a highly iterative process and involves various SMEs and the tight coordination of the Integrated Program Management Team (IPMT). There are two main factors, namely time and budget, which could potentially influence the fidelity of the proposed mitigation measures. For example, the end user will have a pre-determined schedule for the Initial Operational Capability (IOC) for their systems to be introduced into service, which the IPMT have to adhere to strictly. In addition, depending on the acquisition strategy adopted for that particular system, mitigation measures normally may relate to either hardware or software modifications, which may not be catered in the budget upfront.

With the above considerations on the time and budget factors, several trade-off analyses could also be conducted here in order to determine the most feasible and efficient mitigation measures to adopt, for example conducting simulation runs versus

creating actual tests or trials to confirm that mitigation measures are indeed effective in reducing the risks. Nonetheless, it is unavoidable that a certain level of testing will be required as part of the mitigation measures. Therefore, the IPMT also needs to look into the details of how to formulate and create test cases (for example, a thorough series of robustness and endurance tests) for these safety-related hazards so that risks are progressively mitigated with increasing confidence levels.

Create Traceability – From the test cases formulated in the Mitigate function, a database or table of identified risks, described as a Hazard Listing, and its associated mitigation measures should then be created, maintained and tracked conscientiously throughout this whole process. Information in this database should include details such as description of risk, source of risk (Contributing System), affected interfacing systems, initial risk level, consequences, mitigation measures and mitigated/residual risk level.

All safety-related problems observed, whether identified earlier or newly discovered, should be registered during all testing. These problem register log files should also be maintained and subsequently used in the generation of the final safety report. Finally, this database will be useful in providing constant updates to the higher management as well as the end users in terms of number of risks, overall risk level of the large-scale systems integration and progress updates on the mitigation measures for each risk.

Gain Acceptance – This phase describes the residual/mitigated risk review and appraises all stakeholders on the acceptance of all safety hazards associated with the large-scale systems integration. In addition to the Hazard Listing, a risk assessment matrix should also be developed to better represent the associated residual risks in relation to the probability of occurrence, which is dependent on the concept of operations. Therefore, command decisions and the proposed way ahead on whether the residual risks presented will be accepted, or further improvement on the mitigation measures, could be obtained in this phase. Similarly, this function is understood to be an iterative process depending on the criticality of the residual risks presented and the time as well as budget availability whereby the end users may request further mitigation measures to be in place or further testing to be conducted so as to have higher confidence in the residual risks.

This section of the thesis ends with the formulation of the functional hierarchy required for the system safety assessment. In the next section, the measures of effectiveness (MOEs) in terms of key areas of focus will be identified and further described in detail.

THIS PAGE INTENTIONALLY LEFT BLANK

V. KEY FOCUS AREAS FOR CONDUCTING SYSTEM SAFETY ASSESSMENT

A. IDENTIFICATION OF THREE KEY AREAS OF FOCUS

In order to achieve the desired detailed analysis on system safety, three main area of focus for the system safety assessment of large-scale systems integration during its life cycle are presented below. These three focus areas are then further broken down into details and information to consider for each area so that the adequacy of system safety assessment could be efficiently quantified. The three focus areas are:

- Safety to Interfacing Platform
- Safety to Personnel and Operator Handling the System
- Safety Template Optimization

B. SAFETY TO INTERFACING PLATFORM

The first focus area covers system safety in relation to the interfacing platform on which all the systems are to be operated. All safety related issues with regard to inter-systems operations and procedures, as well as their physical integration on these platforms, should be examined. In this aspect, there are generally three sub-areas on which to focus, namely:

1. Operational Usage of Systems with Interfacing Platform

This concerns safety related information on Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) within large-scale systems integration (e.g., radar frequencies versus tactical and exercise missile frequencies). A common reference to be adopted could be MIL-STD-461E [14], which documents the EMI requirements for a wide range of applications, from trucks to ships to aircraft to fixed installations, not to mention the different requirements within an application (e.g., above deck and below deck on a Navy ship). Although most weapon systems are compatible with MIL-STD-461E, it does not necessary imply that they can ‘co-exist’ with other RF radiating systems, such as the surveillance radar.

In most situations, the high transmission power of the ship's radar system will burn out most electronics within its arc of scanning. Thus, it is important to consider the location of ammunition storage onboard as well as the position of launchers with respect to the radar transmission area of arc during integration review meetings to ensure and determine the best course of action to minimize such interference either through design or by procedural means.

2. Operational Profile of Large-scale Systems Integration

In general, this aspect is unique to each country's armed forces' operational concept and war-fighting procedures. Hence, this is very dependent on the nature and environment with which the systems are interfaced based on the desired operation needs. One example is a network connection via Ethernet or dedicated point-to-point connection. In most situations, these connections will be dependent on how the Command and Control (C2) system is to be implemented. In the case example of the Harpoon Weapon System, one possible scenario is to interface with the C2 in a network Ethernet, but with the critical ship's position and dynamics data (roll, pitch, yaw) directly connected to the ship's Inertial Navigation System (INS). With better understanding of the various critical connections and the nature of the backbone and supporting network architecture adopted, it will then be possible to analyze all safety critical events that could lead to undesired consequences; an example is an inadvertent launch of missile during engagement or engaging the wrong target.

3. Structural Integrity

This is a safety study on all physical integration of the systems with the interfacing platform. In general, the interfacing platform will have a set of operational requirements to meet. For example, in the case of a typical warship, it will have the operational requirement that all systems aboard be survivable (able to sustain one underwater shock or explosion) up to sea state 7 and operational (ability to maintain self-defense capability) up to sea state 5.

In addition to these operational requirement considerations, the final design of the platform should also take into account the various Environmental Qualification Tests

(EQT) reports obtained from various systems that will be interfaced onboard. As such, this is one area that needs to be sorted out as early in the life cycle as possible, so that adequate mechanical enhancements to either the platform or to the affected systems, such as additional shock mounts or steel reinforcement implemented on the deck or equipment end, could be finalized after successful integration design review.

Another potential safety-critical pitfall to consider could involve a scenario whereby EQT report suggests that the Harpoon Weapon System launchers are able to sustain two consecutive hang-fires, meaning that the ignition chain and booster are activated, the missile fails to launch and a sustained plume from the booster occurs for a period of time. From the platform structure integrity point of view, it will be difficult to quantify and measure if such an event will cause any severe damage or deformation to the area around the launcher.

Similarly, such critical events should be identified upfront so that further simulation studies or a land-based trial on a mock-up of the platform structure could be conducted to substantiate this safety critical event. Nonetheless, this is one area of platform safety information that will subsequently be propagated downstream into the O&S phase. Without such information being recorded, monitored and tracked effectively, it will be difficult for the logistics personnel to plan and prepare the necessary retrofitting requirements when the ship and/or weapon system reaches the milestone for mid-life upgrade or major overhaul.

C. SAFETY TO PERSONNEL

This final area of safety focus concentrates on the day-to-day handling and operation of the systems by trained operators. It should primarily cover potential safety hazards to the personnel such as electromagnetic radiation, high voltage electric shocks and explosives safety.

1. Radiation Hazards (RADHAZ)

RADHAZ describes the hazards of electromagnetic radiation to fuel, electronic hardware, ordnance, and personnel. It basically defines the safety limit and acceptable

area of operation of the platform based on certain pre-determined frequency and power density ranges. With reference to military context, in accordance to Navy regulation NAVSEA OP3565/NAVAIR 16-1-529 [19 and 20], these hazards are segregated as follows:

- Hazards of Electromagnetic Radiation to Personnel (HERP)
- Hazards of Electromagnetic Radiation to Ordnance (HERO)
- Hazards of Electromagnetic Radiation to Fuel (HERF)

The main reason that this particular safety study is categorized under safety to personnel is the fact that personnel are more vulnerable to these electromagnetic radiation hazards. It literally means that the consequences of HERO and HERF, such as electrical current surge and fire, impose danger to the platform as well as to the personnel. In the context of large-scale systems integration, especially with systems containing explosives and fuel contents, it is thus important to conduct a RADHAZ mapping on the interfacing platform.

The result of the RADHAZ mapping not only sectorizes the safety boundaries on the platform but also determines the level of risks associated with the total number of hazards onboard. This information will further aid the end user in defining and refining his operational profile as well as ensuring that procedures are in place to adequately address all these safety concerns.

2. Ammunition Stowage and Onboard Storage Hazards

This is considered to be one of the major safety concerns in the assessment, as this safety event will potentially impact both the platform and its personnel. Basically, this safety event analysis should cover all aspects of ammunition handling, which first include loading and unloading of ammunition onboard the platform and a review of the maximum height of the ammunition storage in the event of accidental drop (this needs to be correlated to the All-Up round drop tests qualified, for example, up to forty feet height with respect to the waterline). With this information gathered, it will then be easier to devise the plan and procedure to conduct loading and unloading operations with detailed consideration such as wharf position, wind conditions and crane height limitation.

Once ammunition is loaded and stored onboard, another factor to consider will be the quantity and arrangement of this ammunition with respect to other potential ammunition mixes onboard. This leads to another factor to consider in terms of Net Explosive Quantity (NEQ), also known as net explosive content (NEC) or net explosive weight (NEW) [17]. It is defined as the total mass of the contained explosive substances, without the packaging, casings and bullets and includes the mass of the TNT equivalent of all contained energetic substances. This is clearly one of the most critical safety events to consider in detail as the consequences of inadvertent mass detonation of ammunition onboard will be catastrophic.

D. SAFETY TEMPLATE OPTIMIZATION

When there are two or more integrated weapon systems, there is high possibility of overlapping weapon damage areas or what is sometimes known as a violation of weapon safety template of boundaries. In general, the safety template for each weapon or missile is generated or derived based on its associated guidance error as well as other environmental and weapon system consideration. Similarly, these safety templates are again generated based on certain assumptions on the area of operations for the country of origin. Therefore, from the perspective of a COTS/NDI user, there could be further environmental constraints and operational usage that are different from the assumptions used in the safety template generated.

As such, having a clear safety template for each weapon system within the large-scale systems integration will be important in further determining and optimizing the overall large-scale systems safety template. In addition, adherence to the safety template usually requires that certain instrumentation and tracking equipment be in place, such as telemetry equipment, chase aircraft and radar tracking. Therefore, by having a clearer and detailed knowledge of the safety template assumptions for each weapon and missile concerned, both the environment and the resources could all be better optimized for subsequent OT&E live firing events, which will usually mark an important milestone in declaring the system operational.

E. PROPOSED HAZARD LIST TABLE

Based on the above three focus areas, a proposed layout of a hazard list table is described below, with the intent to be able to capture, monitor and trace all safety hazards identified and mitigated throughout the large-scale systems integration life cycle. Using the case example of the SSM System (with Harpoon Weapon System as the lead system), a detailed process of creating this hazard list table is described as follows.

1. Case Example of Safety Assessment of SSM System

From the perspective of a FMS customer, as highlighted earlier the Harpoon Weapon System (HWS) will be procured as a COTS/NDI by foreign armed forces. Typically, as part of the FMS procurement, a safety assessment report for the HWS will be delivered. A summary of the total number of residual risks associated with a standalone Harpoon Weapon System will be provided in the report. For example, there could be X number of Medium risks and Y number of Low risks after safety mitigation factors have been implemented into the design of the system. Table 5 shows an example of a particular safety related hazard identified in the Harpoon Weapon System (HWS) Safety Report [23].

Table 5. Examples of Residual Risks from HWS Safety Report

S/N	Hazard Description	Residual Hazard Risk Index	Mitigation Considerations
1	Inadvertent Launch of Missile	Low	Missile can only be launched with a valid engagement sequence (Safety chain design)
2	Electrocution due to Multiple Sources of Power Supply	Medium	Electric signage on key sub-systems to indicate high voltage hazard

As shown in the above table, there are substantial details that are missing in the summary report, such as the causes of the hazard described, the initial risk when this hazard was identified and any known cases of mishap due to these hazards. In most cases, this information is either proprietary (non-releasable to foreign countries) or simply lost

through the evolution of several system upgrades. Given such constraints and the unknown safety-related problems associated with the weapon system when it is to be integrated on a different platform with different interfacing systems and operating profile, it is important to begin the hazard identification as early as possible in the Integration Design Review (IDR) phase of the COTS/NDI system life cycle, as highlighted in Figure 11 of Chapter III.

From the safety report provided by the Harpoon Weapon System OEM, the IPMT can then initiate the hazard identification as per the functional hierarchy in Figure 14. By considering the three main focus areas described earlier in this section, a SSM System Safety Assessment can be generated as shown in Table 8. With reference to Table 8, considering first the aspect of safety to interfacing platform, the first safety event identified shows that the main mitigation measure to take was procedural control. This in turn had certain implications for the operational readiness of the platform. For example, each time during launch the radar had to be 'switched off' or 'blinded' at certain angles or sectors due to the possibility of 'zapping' the missile prior to launch. This implies that the ship may be limited in self-defense capability during a SSM engagement, which may not be acceptable to the users. Hence, trade-off analysis or further mitigation measures will need to be studied in order to address the operational aspects in relation to this safety event.

The next two safety event examples from Table 8 (S/N 2 & 3 of safety to interfacing platform) described another situation that could possibly occur at different phases of the life cycle. This situation concerns the possibility that there are multiple causes and affected systems associated with a single safety event. In such cases, the safety event should then be broken down in accordance with the affected systems and the different permutations or a series of procedures or operation actions that could lead to the same hazard occurrence. Similarly, the same safety event could be first identified at the IDR stage based on a known series of operations leading to this event, and then during testing phase, the same safety event could occur again but due to another set of operational procedures. Hence, it is important to clearly state the different permutations

and procedures that could lead to the same safety event in the safety hazard table, and then analyze and mitigate each permutation independently.

The final safety event in the safety to interfacing platform area described one situation whereby the structural integrity of the platform and the launcher could be compromised due to the possibility of a hang-fire situation. A certain level of qualification tests on the launcher could have been concluded by Boeing to be able to withstand the plume for a certain duration. However, there could be uncertainty with regard to the structural integrity of the platform in this aspect. Cost will be the main driving factor in determining whether a concise assessment of this safety event could be performed. While simulation analysis could be the most logical and economical approach to take, it will still pale in comparison to performing a mock-up trial for this safety event to find out the actual impact on the platform.

In the next area of safety assessment on personnel, the example provided in Table 8 again shows that a safety event (inadvertent launch) could happen in different modes of the system, such as operational mode versus maintenance. Again, as explained in earlier paragraphs, it is highly recommended to create and assess the effect of different system modes on the same safety event independently. The final safety event in this area was taken directly from the hazard list provided by the OEM as shown in Table 5, above. It is noted that this safety event actually remains exactly the same from its original safety report by OEM as there are no further mitigation measures that could further reduce this risk to a lower level.

The safety assessment for the SSM System described above is an iterative process until all hazards have been determined to be mitigated to a practically reasonable low residual risk. In most cases, this iterative safety assessment will continue until the system successfully completes the OT&E and in preparation to obtain approval from the end users. A typical summary of all residual risks for the SSM System case example may look like Table 6. A total of 3 Medium and 37 Low residual risks have been identified and mitigated as much as possible.

Some conclusions that could be drawn when acquiring final approval from the stakeholder include consideration of the severity of the Medium residual risks combined with their relatively low frequency of occurrence. Therefore, the risks are assessed to be contained and localized with proven mitigation measures put in place. On the other hand, it is also important to take note of the high number of Low residual risk with high frequency of occurrence (Occasional or higher). Although these are the non-significant, non-life threatening safety hazards, they could result in a certain level of operational readiness discomfort if the personnel overlooked these details in day-to-day operations.

Table 6. Case Example Summary for SSM System Residual Risks

Frequency of Occurrence	**Severity**			
	Catastrophic	**Critical**	**Marginal**	**Negligible**
Frequent	-	-	-	-
Probable	-	-	-	-
Occasional	-	-	-	18
Remote	-	2	-	19
Improbable	1	-	-	-

The case example used in this section showed the effectiveness of the safety hazard table in generating, maintaining and tracking all safety events relating to the large-scale systems integration. It is structured with the concept of making it easy to understand for all parties involved, but yet the detailed information collection and analysis to be conducted proved to be the key factors in ensuring that a thorough system safety assessment is performed.

Table 7. Proposed Hazard List Table

SAFETY TO INTERFACING PLATFORM								
S/N	**Hazard Description**	**Affected Systems**	**Initial Hazard Risk Index**	**Life Cycle Phase**	**Mitigation Considerations**	**Final Hazard Risk Index**	**Life Cycle Phase**	**Remarks**
SAFETY TO PERSONNEL								
S/N	**Hazard Description**	**Affected Systems**	**Initial Hazard Risk Index**	**Life Cycle Phase**	**Mitigation Considerations**	**Final Hazard Risk Index**	**Life Cycle Phase**	**Remarks**
SAFETY TEMPLATE OPTIMIZATION								
S/N	**Hazard Description**	**Affected Systems**	**Initial Hazard Risk Index**	**Life Cycle Phase**	**Mitigation Considerations**	**Final Hazard Risk Index**	**Life Cycle Phase**	**Remarks**

Table 8. Case Example of SSM Weapon System Safety Hazard Table

SAFETY TO INTERFACING PLATFORM								
S/N	**Hazard Description**	**Affected Systems**	**Initial Hazard Risk Index**	**Life Cycle Phase**	**Mitigation Considerations**	**Final Hazard Risk Index**	**Life Cycle Phase**	**Remarks**
1.	Electronics burn-out due to EMI from radar	Harpoon Weapon System (HWS)	Low-Medium	IDR	a. Procedural Control (prevent radar operation during missile launch) b. Conduct EMI testing onboard to determine area to sector out during launch.	Low	ICIT	Operational Impact
2.	Inadvertent Launch of Missile (Operational)	HWS, C2 system	Low-Medium	IDR	a. The system design had implemented adequate safety interlocks that prevent this event from occurring. b. Test cases related to this event are thoroughly tested during Integration Testing, FAT and ICIT with no abnormalities observed.	Low	ICIT	
		Ship Power Supply to Launcher	Medium	IDR	a. Procedural Control (Do not connect ignition cable prior to firing)	Low	FAT	
3.	Engage Wrong Target – Different Target numbering reference between HWS and C2	HWS, C2 System and Target Reporting Platform	Medium	IDR	a. Show both C2 Target Number and HWS Track number in one Tactical Picture b. Test cases to be implemented in FAT, Integration Tests and ICIT	Medium	ICIT	
4.	Impact of Sustained Booster Plume due to hang-fire on platform	HWS launchers, deck area	Medium	IDR	a. Simulation runs and mock-up trials to determine weak links in the platform and launcher b. Inspection of Launcher and platform after X number of launches c. Implement local reinforcement	Medium	ICIT	
SAFETY TO PERSONNEL								
S/N	**Hazard Description**	**Affected Systems**	**Initial Hazard Risk Index**	**Life Cycle Phase**	**Mitigation Considerations**	**Final Hazard Risk Index**	**Life Cycle Phase**	**Remarks**
1.	Electric Shock	Harpoon Weapon System, Ship Power Supply	Medium	IDR	a. Electric signage on key sub-systems to indicate high voltage hazard	Medium	IDR	
2.	Inadvertent Launch of Missile (Maintenance)	Harpoon Weapon System, C2 system	Medium	IDR	a. Procedural Control (Do not connect ignition cable prior to firing)	Low	FAT	

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDATIONS AND CONCLUSIONS

A. GENERAL GUIDELINES PROPOSED

This thesis explored the current gaps and potential pitfalls in formulating the system safety assessment for large-scale systems integration, particularly on using and interfacing multiple COTS/NDI systems to fulfill the intended operational requirements. In summarizing the findings gathered in this research, the following guideline and/or checklist attempt to provide a quick overview and template necessary in order to kick-start the system safety assessment.

1. Determining the Lead System Safety Assessment (aka System Integrator)

In order to fulfill the need for a joint weapon safety oversight, it is important first to identify which sub-system within the large-scale systems integration will be the lead system. However, in most cases the logical candidate for the lead system is the weapon system, if it is the only weapon system within the large-scale systems integration. This is due to the fact that the weapon system as compared to other sub-systems, such as the command and control system and sensor system, poses more risks with higher hazard consequences. In contrast, this may not necessarily be true if there is more than one weapon system on multiple platforms within the large-scale systems integration.

To complicate the situation further, each weapon system has its own current stakeholder in their respective Services, as highlighted in Figure 12. It is therefore of utmost importance that the working group formation will involve all stakeholders concerned in the large-scale systems integration. All contributing factors and considerations should be put in place in determining the lead system role collectively.

2. Review of Safety Assessment Matrices

Due to the complexity of the large-scale systems integration of COTS/NDI, there could be a possibility that the Probability of Occurrence in the safety matrix of all the systems could be different and thus need to be reconciled into a standardized matrix. The

MIL-STD-882 as adopted by DoD should be used as much as possible. However, as the probability of occurrence is somehow related to the operational profile/usage determined by different nation's armed forces, there could be further need to look into the system usage in detail and possibly tailor the MIL-STD-882 to suit individual operational requirements. Similarly, the working group for the system safety assessment will provide the right environment and proper guidance in deciding on the eventual risk matrix adopted for the large-scale systems integration.

3. Incorporating Adequate Testing for All Safety Critical Events

Once the initial table of hazard lists is generated during the Integration Design Review stages in the System Acquisition Management phase (refer to Figure 11), it is appropriate to begin to prepare and formulate the test plan for all safety critical events identified. As highlighted in this research, the main mitigation factor for ensuring safety for COTS/NDI systems is to plan and perform more testing before system fielding and operation. Progressive testing should be recommended and incorporated between the Factory Acceptance Tests (FATs) and ICIT, as referenced in Figure 11.

Additionally, because of the complexity in the large-scale systems integration, it is beneficial to set up a laboratory test-bed for integration testing. This should ideally be done before the FATs and after the Final Integration Design Review (FIDR) is completed. Therefore, all safety critical test cases can adequately be created and tested in a controlled environment before deploying the system for field use and trials. Successful completion of this Integration testing phase not only enhances confidence in the systems but also provides all parties with a reference point and minimum threshold level in terms of the system safety readiness before embarking on the subsequent phases.

As the systems go through the Transition to O&S phase of the life cycle, there could be additional integration problems as well as safety-related issues. The laboratory test bed created in the earlier phase will come in handy, as it provides a good avenue to replicate the symptoms encountered in the field during laboratory test cases, in order to

aid further testing and analysis of the problem. Once again, all this information and safety related problems are logged and traced throughout the life cycle within the hazard list table (refer to Table 5) generated earlier.

With all these measures and the necessary tools available, a certain level of confidence could be achieved leading up to the OT & E milestone. Generally, live firing test(s) will be planned at the end of this OT & E phase. The successful completion of the live firing test(s) will provide a better indication to all stakeholders that the system is safe for operational use. In addition, the completion of this milestone further assures that the system safety related information and process have been put in place such that it can be continued to be monitored and traced in the subsequent phases of the system's life cycle until it is retired, disposed of or undergoes further upgrades.

B. CONCLUDING SUMMARY

This thesis research successfully identified the current gap in system safety assessment for large-scale system integrations, especially in the area of COTS and NDI systems integration. A tailored COTS/DNI system integration life cycle process model was determined by referencing the DoD system life cycle process. With this process model created and using a case example of SSM System architecture with the Harpoon Weapon System (HWS) as the lead system, a system safety functional hierarchy was produced. Finally, on the basis of the functional hierarchy, three areas of focus for an effective safety assessment were identified, namely safety to interfacing platform, safety to personnel and safety template optimization.

While current DoD policy considers a joint weapon system safety review board essential, an important further recommendation is to identify the need for an IPMT, as well as a working group, that are essential to oversee the task of safety assessment of large-scale cross-service safety events. A potential pitfall identified in this aspect of multiple system integration is to determine a lead system that will have the overall responsibility to prepare and appraise the end users of the final residual risks for the entire large-scale systems integration. Usually, this lead role is taken up by the weapon system due to the higher risk profile in terms of severity and probability of occurrence.

However, in the event of multiple weapon systems available within the large-scale systems integration, a collective decision making method could be used.

Finally, a hazard list table was proposed as a tool to be used in relation to the system safety assessment functional hierarchy so as to achieve the objective to identify, mitigate, trace and accept all residual risks associated with the large-scale system integration throughout its life cycle. A case example of the SSM System safety assessment on a ship platform was used to further explain the usage and process of generating, maintaining and tracking the hazard list table.

System Safety assessment is very difficult. Without a concise process and architecture as a baseline, it is nearly impossible to conduct effectively a system safety assessment for large-scale systems integration. The Hazard List Table format proposed is a useful tool and provides the necessary information and details necessary to be able to pull out any hazard identified, note when it was surfaced, target mitigation measures to be taken and finally identify the associated residual risk, at any phase of the large-scale systems integration life cycle.

LIST OF REFERENCES

[1] Andrew P. Sage and James E. Armstrong, "Introduction in Systems Engineering," New York: John Wiley & Sons, 2000.

[2] Dennis M. Buede, "The Engineering Design of Systems," New York: John Wiley & Sons, 2000.

[3] William P. Rogers, "Introduction to System Safety Engineering," New York: John Wiley & Sons, 1971.

[4] Jerome Lederer, "How Far Have We Come? A Look Back at the Leading Edge of System Safety Eighteen Years Ago," *Hazard Prevention*, 1986.

[5] Nancy Leveson, "White Paper on Approaches to Safety Engineering," 23 April 2003.

[6] Department of Defense, "Standard Practice for System Safety – MIL-STD-882D," 10 February 2000.

[7] Department of Defense, "Joint Systems Safety Review Guide for USSOCOM Programs," Version 1.1, 12 October 2007.

[8] Department of Defense, "System Safety – ESOH Management Evaluation Criteria for DoD Acquisition," Version 1.1, January 2007.

[9] Department of Defense, "System Safety – ESOH Management Evaluation Criteria for DoD Acquisition," Version 1.1, January 2007.

[10] Robert E. Smith, CSP, "Update on Revisions to MIL-STD-882." NDIA 11th Annual Systems Engineering Conference System Safety – ESOH & HSI Session 3C4, San Diego, CA, 22 October 2008.

[11] APT Research Inc., "System Safety Metrics Method Final Report," Doc. No. S-07-0040, 24 January 2008.

[12] Mark W Maier & Eberhardt Rechtin, "The Art of Systems Architecting – Second Edition," Florida: CRC Press LLC, 2002.

[13] Gregory S. Parnell, Patrick J. Driscoll & Dale L. Henderson, "Decision Making in Systems Engineering and Management," Wiley Series in Systems Engineering and Management, New York: John Wiley & Sons, 2008.

[14] Department of Defense Interface Standard, "Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment – MIL-STD-461E," 20 August 1999.

[15] Memorandum, Secretary of Defense, “Reducing Preventable Accidents,” 19 May 2003.

[16] Memorandum, Under Secretary of Defense for Personnel and Readiness, “Reducing Preventable Accidents,” 11 June 2003.

[17] Allied Ammunition Storage and Transportation Publication, “Manual of NATIO Safety Principles for the Storage of Military Ammunition and Explosives,” May 2006.

[18] Department of Defense Interface Standard, “Electromagnetic Environmental Effects for Systems – MIL-STD-464,” 18 March 1997.

[19] NAVSEA OP 3565/NAVAIR 16-1-529 VOLUME 1 SIXTH REVISION Technical Manual, “Electromagnetic Radiation Hazards (Hazards to Personnel, Fuel and other Flammable Material),” 15 July 1982.

[20] NAVSEA OP 3565/NAVAIR 16-1-529 VOLUME 2 FIFTEEN REVISION Technical Manual, “Electromagnetic Radiation Haz66ards (Hazards to Ordnance),” 1 August 2006.

[21] Professor Thomas Hoivik, USN (Ret), Curriculum OA4603 Test and Evaluation Module, Naval Postgraduate School – Operations Research, September 2009.

[22] Boeing – Integrated Defense Systems, Overview of Harpoon System. Available at http://www.boeing.com/defense-space/missiles/harpoon/docs/HarpoonBlockIIBackgrounder.pdf (last accessed 16 December 2009).

[23] Boeing-McDonnell Douglas, Advanced Harpoon Weapon Control System Safety Report, AHWCS-SAF-SAR-011, 18 December 2003.

INITIAL DISTRIBUTION LIST

1. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

2. Graduate School of Engineering and Applied Sciences
   Naval Postgraduate School
   Monterey, California

3. Professor Eugene Paulo
   Naval Postgraduate School
   Monterey, California

4. Professor and Chairman Clifford Whitcomb
   Naval Postgraduate School
   Monterey, California

5. Tong Choon Yin
   Naval Postgraduate School
   Monterey, California